Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A Virtual Private Network (VPN) communication method employed for a security gateway apparatus connecting between a local area network (LAN) and a wide area network (WAN) including a public network, the communication method comprising the steps of:

a) assigning a first IP address to a terminal outside said LAN;

b) adding a Dynamic Host Configuration Protocol (DHCP) communication option to an Internet Key Exchange (IKE) data, when establishing an IKE communication with [[a]]said terminal outside the LAN having a connection with the WAN;

c) assigning a second IP address from an inside terminal within the LAN to the terminal outside the LAN during the IKE communication, said second address ~~independent~~regardless of said first address; and

d) establishing a Security Architecture for the Internet Protocol (IPsec) communication that follows the IKE communication, which includes said first IP address and said second IP address,

wherein the gateway apparatus designates the first IP address for the outside terminal from a tunneled IP packet.

2. (Original) The VPN communication method employed for the security gateway apparatus as defined in claim 1, wherein an IP address and a subnet mask address, which have same segments as those of the LAN, are distributed to the outside terminal, thereby the outside terminal can be virtually regarded as a terminal on the LAN.

3. (Original) The VPN communication method for the security gateway apparatus as defined in claim 1, wherein the outside terminal is provided, during the IKE communication, with a private IP address that is used on the LAN, in a case that the LAN is configured with private IP addresses, whereby the outside terminal is allowed to access to a terminal on the LAN.

4. (Previously Presented) The VPN communication method for the security gateway apparatus according to claim 1, wherein an encryption key and an authentication key are exchanged with a public key cryptosystem during the IKE communication.

5. (Previously Presented) The VPN communication method for the security gateway apparatus according to claim 1, wherein the DHCP communication option contains an IP address and a subnet mask.

6. (Currently Amended) A security gateway apparatus connecting between a local area network (LAN) and a wide area network (WAN) including a public network, the apparatus comprising:

a) a Dynamic Host Configuration Protocol (DHCP) option adding section adding a DHCP communication option to an IKE data when establishing an IKE communication with [[a]]an outside terminal having a first IP address distributed from outside the LAN having a connection with the WAN;

b) an IP address distribution section assigning a second IP address from an inside terminal within the LAN to the outside terminal during the IKE communication, said second address ~~independent~~regardless of said first address; and

c) an IPsec communication section performing an IPsec communication that follows the IKE communication, which includes said first IP address and said second IP address,

wherein, the gateway apparatus designates the first IP address for the outside terminal from a tunneled IP packet.

7. (Original) The security gateway apparatus as defined in claim 6, wherein an IP address and a subnet mask address, which have same segments as those of the LAN, are distributed to the outside terminal, thereby the outside terminal can be virtually regarded as a terminal on the LAN.

8. (Original) The security gateway apparatus as defined in claim 6, wherein the outside terminal is provided, during the IKE communication, with a private IP address which is the same as one used on the LAN in a case that the LAN is configured with private IP addresses, whereby the outside terminal is allowed to access to a terminal on the LAN.

9. (Previously Presented) The security gateway apparatus according to claim 6, wherein an encryption key and an authentication key are exchanged with a public key cryptosystem during the IKE communication.

10. (Previously Presented) The security gateway apparatus according to claim 6, wherein the DHCP communication option contains an IP address and a subnet mask.

11. (Previously Presented) The VPN communication method for the security gateway apparatus according to claim 2, wherein an encryption key and an authentication key are exchanged with a public key cryptosystem during the IKE communication.

12. (Previously Presented) The VPN communication method for the security gateway apparatus according to claim 3, wherein an encryption key and an authentication key are exchanged with a public key cryptosystem during the IKE communication.

13. (Previously Presented) The VPN communication method for the security gateway apparatus according to claim 2, wherein the DHCP communication option contains an IP address and a subnet mask.

14. (Previously Presented) The VPN communication method for the security gateway apparatus according to claim 2, wherein the DHCP communication option contains an IP address and a subnet mask.

15. (Previously Presented) The security gateway apparatus according to claim 7, wherein an encryption key and an authentication key are exchanged with a public key cryptosystem during the IKE communication.

16. (Previously Presented) The security gateway apparatus according to claim 8, wherein an encryption key and an authentication key are exchanged with a public key cryptosystem during the IKE communication.

17. (Previously Presented) The security gateway apparatus according to claim 7, wherein the DHCP communication option contains an IP address and a subnet mask.

18. (Previously Presented) The security gateway apparatus according to claim 8, wherein the DHCP communication option contains an IP address and a subnet mask.

19. (Previously Presented) The VPN communication method employed for the security gateway apparatus as defined in claim 1, wherein said terminal outside the LAN has a dialup connection with the WAN.

20. (Previously Presented) The VPN communication method employed for the security gateway apparatus as defined in claim 1, wherein said second IP address is automatically distributed from the terminal within the LAN to the terminal outside the LAN during the IKE communication.

21. (Previously Presented) The security gateway apparatus as defined in claim 6, wherein said terminal outside the LAN has a dialup connection with the WAN.

22. (Previously Presented) The security gateway apparatus as defined in claim 6, wherein said second IP address is automatically distributed from the terminal within the LAN to the terminal outside the LAN during the IKE communication.

23. (Currently Amended) A VPN communication method according to claim 1, wherein said first IP address is assigned to said terminal from outside said LAN.

24. (New) A security gateway apparatus according to claim 6, wherein said first IP address is assigned to said terminal from outside said LAN.